INDUSTRIAL PROCESS CONTROL SYSTEM WORKSHOP

APRIL 19-20, 2006

NATIONAL INSTITUTE FOR STANDARDS AND TECHNOLOGY

GAITHERSBURG, MD

MEETING MINUTES

FACILITATOR:	NIST – Stu Katzke, Keith Stouffer	**DATE:**	Wednesday, April 19, 2006
SCRIBE:	Hussain Jafri	**TIME:**	09:00 – 17:00
HANDOUTS:	Agenda, Background Invitation Letter & Details letter, 800-53 R1 Draft	**LOCATION:**	NIST Main Campus Shops Bldg 304 Room B126

This document is a work-in-progress, is being shared through a limited distribution, and may not be quoted, referenced, or redistributed without NIST's permission.

1. Wednesday, April 19, 2006

I. Welcome & Introduction to Industrial Process Control Systems (ICS) and Supervisory Control & Data Acquisition (SCADA) Workshop

a. Identification of short and long term goals.

b. Overview of Federal Information Systems Management Act (FISMA) with respect to ICS and SCADA systems.

c. Presented National Institute for Standards and Technology (NIST) accomplishments assisting federal agencies to meet FISMA requirements (i.e. NIST Special Publication 800-53).

d. Joint project has been established between NIST's Intelligent Systems Division (ISD) (in the Manufacturing Engineering Lab (MEL)) and the Computer Security Division (CSD) (in the Information Technology Lab (ITL)) to improve the security of public and private Industrial Control Systems (ICS).

e. FISMA required NIST to develop standards and guidelines

f. Development of Federal Information Processing Standards (FIPS) 199 & 200

g. Development of Credentialing Program – To certify organizations offering C&A services

h. Special Publication (SP) 800-53A – Guide for Assessing the Security Controls in Federal Information Systems second public draft to be released April 21

II. Presentation on mapping of NERC CIP and 800-53 Revision 1

a. All of the NERC CIP requirements in some form or fashion map to 800-53 controls and/or countermeasures.

b. Not all controls and/or countermeasures in the 800-53 map to the NERC CIP

c. 800-53 is a superset of the NERC CIP

This document is a work-in-progress, is being shared through a limited distribution, and may not be quoted, referenced, or redistributed without NIST's permission.

2. Discussion Items

Item	Discussion
NIST SP800-53	➢ **NIST SP800-53 Recommended Security Controls for Federal Information Systems Revision 2 will be available in May 2006. Results from ICS Workshop can be included.**
FERC	➢ **Federal Energy Regulatory Commission (FERC) will be requesting comments on the North American Electric Reliability Council (NERC) Critical Infrastructure Protection (CIP), available on the FERC website in early May.**
Jurisdiction of Compliance for ICS Industry	➢ **Various organizations claim that ICS systems do not fall under FISMA regulations. There is no clear language that says ICS systems must comply with the various government regulations regarding the FISMA compliance.** ➢ **This is a major issue and needs to be addressed.**
Auditing	➢ **Auditors need to be better trained in conducting audits specifically for ICS systems.** ➢ **DHS is trying to develop metrics to help in this arena.** ➢ **A guide should be developed specifically for auditors (e.g.,. a Special Publication).**
System Categorization	1. **The current categorization system is not well understood and/or is not being applied consistently. Additional guidance may be needed on how to apply FIPS 199 to Industrial Control Systems. As it stands now, the categorization is not being done correctly by the first line implementers.** 2. **There is significant variation/inconsistency in the way agencies are applying FIPS 199 to ICS's. The variations/inconsistencies are occurring from agency to agency and within agencies. For ICS's, the agencies are having difficulty assessing the effective impact of a security failure because the impact to the organization mission, etc. is not always the same as the impact to the critical infrastructure that the system is attached to or is part of.** 3. **All ICS's considered to be part of the government's critical infrastructure should be categorized as "at least moderate" and hence must apply the corresponding security control baseline until it is determined otherwise.** 4. **Business Impact Assessments may be one solution to help better determine categorization. Business Impact Assessment appears in SP 800-34 Contingency Planning Guide for Information Technology Systems – Appendix B: Business Impact Analysis and BIA Template.** 5. **It is believed by many in the industry that the ISO 17799 and NIST Business Impact Assessment conflict each other.** Its not clear what that means. It appears to be comparing apples and oranges. ISO 17799 is a catalog of countermeasures (like SP 800-53). Further information will help us understand.
Review of SP800-53 Release 1 Controls for ICS Systems	➢ **Selection of SP800-53 Revision 1 Controls/Countermeasures that need to be discussed with regards to their impact on ICS systems (See Section 3 below – SP800-53 Revision 1 Controls voting).** o **Rules for voting:** ▪ **Yes – It will be discussed tomorrow (number of votes in parenthesis)** ▪ **No – The control is okay**

This document is a work-in-progress, is being shared through a limited distribution, and may not be quoted, referenced, or redistributed without NIST's permission.

3. 800-53 Revision 1 Controls Voting

AC-1	ACCESS CONTROL POLICY AND PROCEDURES	NO
AC-2	ACCOUNT MANAGEMENT	YES 7
AC-3	ACCESS ENFORCEMENT	YES 10
AC-4	INFORMATION FLOW ENFORCEMENT	NO
AC-5	SEPARATION OF DUTIES	YES 11
AC-6	LEAST PRIVILEGE	YES 8
AC-7	UNSUCCESSFUL LOGIN ATTEMPTS	YES 12
AC-8	SYSTEM USE NOTIFICATION	YES 2
AC-9	PREVIOUS LOGON NOTIFICATION	YES 3
AC-10	CONCURRENT SESSION CONTROL	YES 12
AC-11	SESSION LOCK	YES 12
AC-12	SESSION TERMINATION	YES 12
AC-13	SUPERVISION AND REVIEW — ACCESS CONTROL	YES 3
AC-14	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	YES 6
AC-15	AUTOMATED MARKING	YES 4
AC-16	AUTOMATED LABELING	YES 2
AC-17	REMOTE ACCESS	YES 6
AC-18	WIRELESS ACCESS RESTRICTIONS	YES 7
AC-19	ACCESS CONTROL FOR PORTABLE AND MOBILE DEVICES	YES 10
AC-20	PERSONALLY OWNED INFORMATION SYSTEMS	NO
AT-1	SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES	NO
AT-2	SECURITY AWARENESS	YES 1
AT-3	SECURITY TRAINING	YES 1
AT-4	SECURITY TRAINING RECORDS	NO
AT-5	CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS	NO
AU-1	AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES	NO
AU-2	AUDITABLE EVENTS	YES 6
AU-3	CONTENT OF AUDIT RECORDS	YES 3
AU-4	AUDIT STORAGE CAPACITY	NO
AU-5	AUDIT PROCESSING	NO
AU-6	AUDIT MONITORING, ANALYSIS, AND REPORTING	YES 4
AU-7	AUDIT REDUCTION AND REPORT GENERATION	NO
AU-8	TIME STAMPS	NO
AU-9	PROTECTION OF AUDIT INFORMATION	YES 1
AU-10	NON-REPUDIATION	YES 8
AU-11	AUDIT RETENTION	NO
CA-1	CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENT POLICIES AND PROCEDURES	NO
CA-2	SECURITY ASSESSMENTS	YES 6
CA-3	INFORMATION SYSTEM CONNECTIONS	YES 1
CA-4	SECURITY CERTIFICATION	YES 3
CA-5	PLAN OF ACTION AND MILESTONES	NO
CA-6	SECURITY ACCREDITATION	NO
CM-1	CONFIGURATION MANAGEMENT POLICY AND PROCEDURES	NO
CM-2	BASELINE CONFIGURATION AND SYSTEM COMPONENT INVENTORY	YES 6
CM-3	CONFIGURATION CHANGE CONTROL	YES 1
CM-4	MONITORING CONFIGURATION CHANGES	YES 1
CM-5	ACCESS RESTRICTIONS FOR CHANGE	YES 2
CM-6	CONFIGURATION SETTINGS	YES 2
CM-7	LEAST FUNCTIONALITY	YES 3
CP-1	CONTINGENCY PLANNING POLICY AND PROCEDURES	NO
CP-2	CONTINGENCY PLAN	NO
CP-3	CONTINGENCY TRAINING	NO

CP-4	CONTINGENCY PLAN TESTING	YES 3
CP-5	CONTINGENCY PLAN UPDATE	NO
CP-6	ALTERNATE STORAGE SITES	NO
CP-7	ALTERNATE PROCESSING SITES	YES 4
CP-8	TELECOMMUNICATIONS SERVICES	NO
CP-9	INFORMATION SYSTEM BACKUP	NO
CP-10	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION	YES 3
IA-1	IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES	NO
IA-2	USER IDENTIFICATION AND AUTHENTICATION	YES 7
IA-3	DEVICE IDENTIFICATION AND AUTHENTICATION	YES 2
IA-4	IDENTIFIER MANAGEMENT	YES 4
IA-5	AUTHENTICATOR MANAGEMENT	YES 3
IA-6	AUTHENTICATOR FEEDBACK	YES 1
IA-7	CRYPTOGRAPHIC MODULE AUTHENTICATION	YES 1
IR-1	INCIDENT RESPONSE POLICY AND PROCEDURES	NO
IR-2	INCIDENT RESPONSE TRAINING	NO
IR-3	INCIDENT RESPONSE TESTING	NO
IR-4	INCIDENT HANDLING	NO
IR-5	INCIDENT MONITORING	NO
IR-6	INCIDENT REPORTING	NO
IR-7	INCIDENT RESPONSE ASSISTANCE	NO
MA-1	SYSTEM MAINTENANCE POLICY AND PROCEDURES	NO
MA-2	PERIODIC MAINTENANCE	YES 2
MA-3	MAINTENANCE TOOLS	NO
MA-4	REMOTE MAINTENANCE	YES 6
MA-5	MAINTENANCE PERSONNEL	NO
MA-6	TIMELY MAINTENANCE	NO
MP-1	MEDIA PROTECTION POLICY AND PROCEDURES	NO
MP-2	MEDIA ACCESS	YES 1
MP-3	MEDIA LABELING	NO
MP-4	MEDIA STORAGE	NO
MP-5	MEDIA TRANSPORT	NO
MP-6	MEDIA SANITIZATION AND DISPOSAL	NO
PE-1	PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES	NO
PE-2	PHYSICAL ACCESS AUTHORIZATIONS	YES 1
PE-3	PHYSICAL ACCESS CONTROL	YES 2
PE-4	ACCESS CONTROL FOR TRANSMISSION MEDIUM	YES 5
PE-5	ACCESS CONTROL FOR DISPLAY MEDIUM	YES 1
PE-6	MONITORING PHYSICAL ACCESS	YES 1
PE-7	VISITOR CONTROL	NO
PE-8	ACCESS LOGS	YES 1
PE-9	POWER EQUIPMENT AND POWER CABLING	NO
PE-10	EMERGENCY SHUTOFF	NO
PE-11	EMERGENCY POWER	YES 6
PE-12	EMERGENCY LIGHTING	YES 1
PE-13	FIRE PROTECTION	NO
PE-14	TEMPERATURE AND HUMIDITY CONTROLS	NO
PE-15	WATER DAMAGE PROTECTION	NO
PE-16	DELIVERY AND REMOVAL	NO
PE-17	ALTERNATE WORK SITE	NO
PE-18	LOCATION OF INFORMATION SYSTEM COMPONENTS	YES 4
PE-19	INFORMATION LEAKAGE	NO
PL-1	SECURITY PLANNING POLICY AND PROCEDURES	NO
PL-2	SYSTEM SECURITY PLAN	NO
PL-3	SYSTEM SECURITY PLAN UPDATE	NO
PL-4	RULES OF BEHAVIOR	NO

PL-5	PRIVACY IMPACT ASSESSMENT	YES 4
PL-6	SECURITY-RELATED ACTIVITY PLANNING	NO
PS-1	PERSONNEL SECURITY POLICY AND PROCEDURES	NO
PS-2	POSITION CATEGORIZATION	NO
PS-3	PERSONNEL SCREENING	YES 1
PS-4	PERSONNEL TERMINATION	NO
PS-5	PERSONNEL TRANSFER	NO
PS-6	ACCESS AGREEMENTS	NO
PS-7	THIRD-PARTY PERSONNEL SECURITY	NO
PS-8	PERSONNEL SANCTIONS	NO
RA-1	RISK ASSESSMENT POLICY AND PROCEDURES	NO
RA-2	SECURITY CATEGORIZATION	YES 5
RA-3	RISK ASSESSMENT	NO
RA-4	RISK ASSESSMENT UPDATE	NO
RA-5	VULNERABILITY SCANNING	YES 12
SA-1	SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES	NO
SA-2	ALLOCATION OF RESOURCES	NO
SA-3	LIFE CYCLE SUPPORT	NO
SA-4	ACQUISITIONS	YES 1
SA-5	INFORMATION SYSTEM DOCUMENTATION	YES 1
SA-6	SOFTWARE USAGE RESTRICTIONS	NO
SA-7	USER INSTALLED SOFTWARE	YES 1
SA-8	SECURITY DESIGN PRINCIPLES	NO
SA-9	OUTSOURCED INFORMATION SYSTEM SERVICES	YES 2
SA-10	DEVELOPER CONFIGURATION MANAGEMENT	NO
SA-11	DEVELOPER SECURITY TESTING	NO
SC-1	SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES	NO
SC-2	APPLICATION PARTITIONING	NO
SC-3	SECURITY FUNCTION ISOLATION	YES 7
SC-4	INFORMATION REMNANTS	YES 3
SC-5	DENIAL OF SERVICE PROTECTION	YES 4
SC-6	RESOURCE PRIORITY	YES 1
SC-7	BOUNDARY PROTECTION	NO
SC-8	TRANSMISSION INTEGRITY	YES 6
SC-9	TRANSMISSION CONFIDENTIALITY	YES 9
SC-10	NETWORK DISCONNECT	YES 9
SC-11	TRUSTED PATH	YES 8
SC-12	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	YES 1
SC-13	USE OF VALIDATED CRYPTOGRAPHY	YES 1
SC-14	PUBLIC ACCESS PROTECTIONS	NO
SC-15	COLLABORATIVE COMPUTING	YES 1
SC-16	TRANSMISSION OF SECURITY PARAMETERS	NO
SC-17	PUBLIC KEY INFRASTRUCTURE CERTIFICATES	YES 3
SC-18	MOBILE CODE	NO
SC-19	VOICE OVER INTERNET PROTOCOL	NO
SC-20	SECURE NAME LOOKUP SERVICE (AUTHORITATIVE SOURCE)	NO
SC-21	SECURE NAME LOOKUP SERVICE (RESOLUTION)	NO
SI-1	SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES	NO
SI-2	FLAW REMEDIATION	YES 2
SI-3	MALICIOUS CODE PROTECTION	YES 9
SI-4	INFORMATION SYSTEM MONITORING TOOLS AND TECHNIQUES	YES 1
SI-5	SECURITY ALERTS AND ADVISORIES	YES 1
SI-6	SECURITY FUNCTIONALITY VERIFICATION	YES 5
SI-7	SOFTWARE AND INFORMATION INTEGRITY	YES 5
SI-8	SPAM PROTECTION	YES 4
SI-9	INFORMATION INPUT RESTRICTIONS	YES 3

This document is a work-in-progress, is being shared through a limited distribution, and may not be quoted, referenced, or redistributed without NIST's permission.

SI-10	INFORMATION ACCURACY, COMPLETENESS, VALIDITY, AND AUTHENTICITY	YES 2
SI-11	ERROR HANDLING	NO
SI-12	INFORMATION OUTPUT HANDLING AND RETENTION	NO

4. Thursday, April 20, 2006

Review of NIST Special Publication (SP) 800-53 Revision 1 Controls/Countermeasures in Relation to Industrial Control Systems (ICS) and Supervisory Control & Data Acquisition (SCADA) systems. The discussion captured below indicates topics requiring clarification or correction. The statements are not necessarily correct nor are they the NIST position.

800-53 CONTROL	DISCUSSION
AC-2 Account Management	➢ There is an issue with disabling or removing of accounts/passwords that is stated in the Control Enhancement section. In ICS systems Passwords may have to be set manually. The issue is with the term "automated". Most field devices out of the box will not meet these requirements. Also an issue with Control Enhancement, the systems cannot terminate automatically accounts. The accounts in ICS systems may be role-based and device-based with login. ➢ Need to define automated and acknowledge ICS systems have a different set of capabilities than IT systems. IT systems and ICS systems handle account management differently. In many cases the accounts are role-based situations where a workstation defines a role. So defined by the hardware based, physical presence is the access control.
AC-3 Access Enforcement	➢ The issue is similar to AC-2. In the Control Enhancement it states "…information is restricted to authorized personnel". It should state "restricted to workstation" instead. ➢ ICS systems use more role-based systems and use other compensating controls such as: o Enhanced physical controls. o Background investigations o Video surveillance o Authorized users only allowed in area o Escorted visitors/emergency personnel, etc. o Need an access control policy (e.g., repair personnel, IG, firemen)
AC-5 Separation of Duties	➢ ICS systems are not controlled by single-users. If you have access to the control room you have access to the entire system. There is only one password to access the system. Wording in AC-5 needs to be changed to replace "information system" to "Organization". Prevent "unauthorized" users. Need to enhance wording to reflect small organizations and personnel with multiple roles. Need to also note the purpose of control is to avoid conflict of interest.
AC-6 Least Privilege	➢ Same issues as above. ICS systems are mostly role-based systems and thus this does not apply.
AC-7 Unsuccessful login Attempts	➢ This may not work in ICS environments in all cases. You will need a business or risk assessment. In some cases you can only log/record attempts. Supplemental Guidance needs to be clarified. It is a safety issue if personnel are locked out. The guidance should reflect "scoping out" risk and acceptance of that risk. Need to provide examples. If possible just log unsuccessful attempts.

AC-10 Concurrent Session Control	➢ ICS systems or devices may not allow concurrent sessions to be limited. Need better wording in the guidance where organizations cannot abide by this control.

800-53 CONTROL	DISCUSSION
AC-11 Session Lock	➢ This is same issue as AC-7. It is important to do a risk analysis. ➢ In Supplemental Guidance the term "user" needs to be defined.
AC-12 Session Termination	➢ Same issues as AC-7. Need to use better wording. Need to clarify the word "session" is it "user session" or "device session". Need to better define "users", may not always be an individual person, may be a system-to-system connection. Needs to be policy-based.
AC-17 Remote Access	➢ Control Enhancements need to be rewritten (e.g. Need to use enhanced methods or other secure mechanisms to ensure CIA levels). ➢ Need to conduct a risk analysis. ICS field devices cannot use full-blown encryption. May not be able to do monitoring. ➢ Suggestions: ➢ May want to remove "Internet devices" can be people. ➢ To replace #2 – The organization uses enhanced defense mechanisms to protect the remote access sessions. ➢ Take out the word "automated". Remote access might be done manually.
AC-18 Wireless Access Restrictions	➢ Need to better define the term "wireless". Does it include micro or near-microwave length? What types of wireless communications does this refer to? ➢ Defensive mechanisms need to be placed based on risk analysis that narrow down what needs to be protected. ➢ Examples: ➢ Where UHF/VHF signals are used. ➢ There is a difference in opinion in the industry regarding the scope of "wireless" technology. Some believe it is restricted to WiFi and others believe it includes all/other types of wireless communication.
AC-19 Access Control for Portable and Mobile Devices	➢ Control enhancement is too technology specific to protect information. ➢ In supplemental guidance need to change "removable hard drives or cryptography" to "defensive mechanisms". Some information, such as configuration information, should be encrypted but you cannot always due to legacy technology. Organizations need to apply defensive mechanisms to protect removable media (removing "removable hard drives." – This is a big issue because so many attacks have been executed via removable media.
AU-2 Auditable Events	➢ Most ICS systems audit at the application layer. More guidance on what should be captured for auditing (i.e. OS layer, application layer, operational data points, etc.) needed. ➢ The existing checklist referred in the Supplemental Guidance section does not address properly the needs/requirements of the ICS community. ➢ Need to review 800-12 (as referred in AU-1). ➢ Many times auditing refers to database entries and auditing of that type of auditing in SCADA systems will break the system. ➢ The entire AU family needs to be re-examined to better fit ICS industry. Also a new SP needs to be written for AU family.

AU-10 Non-Repudiation	➢ It is not part of any baseline. Some systems may not allow traceability to an individual user, may be group or role.

This document is a work-in-progress, is being shared through a limited distribution, and may not be quoted, referenced, or redistributed without NIST's permission.

800-53 CONTROL	DISCUSSION
CA-2 Security Assessments	➢ Would like to see more guidance on how to conduct testing on SCADA/ICS systems.
CM-2 Baseline Configuration and System Component Inventory	➢ The issue is with the term “complying with the Federal Architecture”. ICS systems are not part of the Federal Architecture. ➢ Would like to see more validation process/procedures in SSP or some where else (as required in DITSCAP). ➢ Need to use the term “if possible” regarding the details of the devices. Some devices may not have serial numbers, part number, etc. ➢ For SCADA systems the term “automated” needs to be better defined. SCADA systems do not always use automated systems.
IA-2 User Identification and Authentication	➢ Goes back to the issue of unique user identification. ICS systems use role-based or group-based ID and Authentication. ➢ The question is raised, is HSPD-12 intended for ICS systems?
MA-4 Remote Maintenance	➢ Supplemental guidance mentions technology and procedures that may be available and/or not be usable, advisable, or practical in ICS (e.g., sanitize and disconnect). ➢ Change wording from “transmission” to “communication” line. Should be differentiation between in-house and third party maintenance.
PE-4 Access Control for Transmission Medium	➢ Issue is the definition of the facility and the potentially wide physical distribution of the facility. Include transmission that is not over a physical media (i.e., controlling access to Satellite Ground Stations, Microwave Towers, etc.). ➢ Change the word “transmission lines” to “communication lines”. ➢ PE-3 refers to physical access to facilities; PE-4 refers to locked wiring closets. It covers protection of satellite ground stations. The focus of PE-4 is to prevent malicious access by making sure the transmission closets are locked and secure. PE-4 is effectively good as is but need to ensure that 800-53 is adequately addressing detection.
PE-11 Emergency Power	➢ Requirement needs to be more robust. For ICSs you want to keep them running, not shut them down. You have to look at the process you are controlling and understand if you need to keep the ICS going for safety reasons. This control allows you to decide what you need to keep running. Should be PE-11 (1) for all levels.
RA-2 Security Categorization	➢ It is difficult to categorize ICS systems same as IT systems. ➢ Business partners need to be a part of the categorization exercise. Need to include “stakeholders” (explain in what context).

800-53 CONTROL	DISCUSSION
RA-5 Vulnerability Scanning	➢ Need to do manual verification versus automated verification. Using automated tools can break ICS systems. ➢ In supplemental documentation there should be some verbiage regarding great concern should be taken before scanning takes place due to the sensitivity of ICS systems. ➢ Need to create a separate document detailing how to scan ICS systems. ➢ The verbiage needs to be very carefully written to not openly share the vulnerabilities of the ICS systems. ➢ Need to change requirement to a manual process where you compare known vulnerabilities to the system's configuration. Should run a vulnerability scan on a test system that is similar to live system. Most SCADA systems are designed to make max use of the processor so a scan would cause a denial of service to the system. ➢ Off the shelf scanners are not designed to scan SCADA configurations. You have to understand how a system will respond to an unusual packet - which is how scanner packets will be perceived by some systems. NIST should develop a supplemental guidance document for ICS scanning.
SC-3 Security Function Isolation	➢ The term "Security Function" is not defined well. It means the security function is on a separate system to not allow someone to access or tamper with the security functions in case of breach of the original system. o Suggestions: ▪ Change high to not selected. ▪ Change hardware separation to "logical separation". ▪ Remove "underline hardware" in enhancement 1. ➢ ICS systems are not designed for security function isolation.
SC-8 Transmission Integrity	➢ IPSEC in supplemental guidance should be taken out. ➢ The issue is by incorporating encryption or cryptographic devices in ICS systems can break the systems. o Suggestions: ▪ Take out the word "cryptographic" for high in control enhancement.
SC-9 Transmission Confidentiality	➢ Same issues as above. ➢ Failure of cryptographic device may cause the loss of data being able to be seen (i.e. loss of control).
SC-10 Network Disconnect	➢ Same as AC-12
SC-11- Trusted Path	➢ Need proper definition for Trusted Path – Means the connection between user and security function is secure. ➢ Same issues as SC-3.

800-53 CONTROL	DISCUSSION
SI-3 Malicious Code Protection	➢ Automatic updates may not work in ICS environments. Updates have to be tested thoroughly and are usually done by the vendor before being incorporated into ICS. o Suggestions: ▪ Should be moved to control enhancement (1) (is debatable).
SI-6 Security Functionality Verification	➢ Same as SC-3. ➢ Control suggests the information system verifies the correct operation of security functions upon shutdown or start-up. Shutting down and restarting ICS systems may not be an option.
SI-7 Software and Information Integrity	➢ The control suggests using tools to automatically monitor the integrity of the systems and applications. Certain ICS systems cannot be done “automatically”. Need to change the verbiage to exclude the term “automatically”. o Suggestions: ▪ Add “to the extent feasible” because it cannot be done currently in many systems.
SI-8 Spam Protection	➢ Because ICS systems run differently than regular IT systems, it is not employ Spam protection mechanisms. Unusual traffic flow such as during crisis situations may be misinterpreted and caught as spam and cause issues with the system and possible failure of the system. ➢ Automatic updates again can be an issue.
SI-9 Information Input Restrictions	➢ Not an issue
SC-17 Public Key Infrastructure Certificates	➢ ICS systems may not want/need or be able to use PKI certificate system.
SC-5 Denial of Service Protection	➢ Same as SI-8
SC-4 Information Remnants	➢ Not applicable to ICS systems
PL-5 Privacy Impact Assessment	➢ Does not apply to ICS systems
PE-18 Location of Information Systems Components	➢ Not an issue
IA-3 Device Identification and Authentication	➢ Not an issue
IA-4 Identifier Management	➢ Same issue as noted before (group and/or role-based operation versus individual operation).

This document is a work-in-progress, is being shared through a limited distribution, and may not be quoted, referenced, or redistributed without NIST’s permission.

IA-5 Authenticator Management	➢ Same issue as noted before (group and/or role-based operation versus individual operation).
800-53 CONTROL	**DISCUSSION**
CP-7 Alternate Processing Site	➢ If for any reason an ICS cannot meet the requirement then there needs to be supplemental guidance on what to do.
CP-10 Information Recovery and Reconstitution	➢ The word “Full” is not applicable in ICS industry.
AC-9 Previous Logon Notification	➢ Not an issue
AC-13 Supervision and Review – Access Control	➢ Field devices do not allow for this. Remove the word Automation.
AC-14 Permitted Actions without Identification or Authentication	➢ Not applicable to ICS industry.
AC-15 Automated Marking	➢ This is primarily used for Confidentiality categorization. Can use tailoring guidance to downgrade.

This document is a work-in-progress, is being shared through a limited distribution, and may not be quoted, referenced, or redistributed without NIST’s permission.

5. Action Items

Action items:	Person responsible:	Deadline:
Write-up general Meeting Minutes	Hussain Jafri	
Write-up notes from second day of meeting – 800-53 Controls Review	Hussain Jafri	
Write-up global issues and provide them for NIST (Stu, Keith & Ron)	Marshall Abrams	

6. Attendees

Name	Title	Organization	Phone Number	E-Mail
Keith Stouffer	Mechanical Engineer	National Institute of Standards & Technology	(301) 975-3877	keith.stouffer@nist.gov
Stu Katzke	Senior Research Scientist	National Institute of Standards & Technology	(301) 975-4768	skatzke@nist.gov
Alicia Clay	Senior Information Security Analyst	National Institute of Standards & Technology	(301) 975-3641	Alicia.Clay@nist.gov
Derrick Moe	Operations Support Manager	Western Area Power Administration	(605) 882-7501	moe@wapa.gov
James Phillips	Network Lead	Western Area Power Administration	(605) 882-7524	JPhillips@wapa.gov
Ken Hollis	Senior Network Manager	Southwestern Power Administration	(918) 595-6737	ken.hollis@swpa.gov
Daniel Bogle	IT Management Specialist	Federal Energy Regulatory Commission	(202) 502-6049	daniel.bogle@ferc.gov
Mike Peters	Energy Infrastructure & Cyber Security Advisor	Federal Energy Regulatory Commission	(202) 502-8461	Michael.Peters@ferc.gov
Steve Yexley	C&A Program Manager	Western Area Power Administration	720-962-7351	Yexley@wapa.gov
Jeff Mantong	Cyber Security Officer	Western Area Power Administration	(916) 353-4513	mantong@wapa.gov
Laurent Webber	Cyber Security Program Manager	Western Area Power Administration	720-962-7216	Webber@wapa.gov
Tom McDowell		Bureau of Reclamation	(720) 253-5437	Tmcdowell@do.usbr.gov
Lee Matuszczak	Bureau IT Security Manager (BITSM)	Bureau of Reclamation	303-445-3718	lmatuszczak@do.usbr.gov

Shabbir Shamsuddin	Energy Systems Analyst	Argonne National Laboratory	(630) 252-6273	shamsuddin@anl.gov
Robert Evans	Cyber Security Standards SCADA & Power Systems Security Resources	Idaho National Laboratory	(208) 526-0852	Robert.Evans@inl.gov
Mary Young	Principal Member of Technical Staff Information Operations Red Team & Assessments (IORTA)	Sandia National Labs	(505) 844-8003	mlyoung@sandia.gov
Thomas G. Peters	Director, Control Systems Security Program	US Department of Homeland Security	(703) 235-5403	Thomas.Peters@dhs.gov
Julio Rodriguez	Strategic Advisor for Control Systems Critical Infrastructure Protection Division	US Department of Homeland Security	(703) 235-5402	Julio.Rodriguez@associates.dhs.gov
Annabelle Lee	Director, Security Standards, Best Practices and R&D Requirements	US Department of Homeland Security	(703) 235-5406	Annabelle.Lee@dhs.gov
Jim Lund		US Department of Energy	(301) 903-1294	James.Lund@hq.doe.gov
Marshall Abrams	Principal Scientist	MITRE	(703) 983-6938	abrams@mitre.org
Hussain Jafri	Senior INFOSEC Engineer/Scientist	MITRE	(443) 717-2136	hjafri@mitre.org

This document is a work-in-progress, is being shared through a limited distribution, and may not be quoted, referenced, or redistributed without NIST’s permission.